

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

NATHAN COLOMBO, *individually and on
behalf of all others similarly situated,*

Plaintiff,

v.

YOUTUBE, LLC, et al.,

Defendants.

Case No. [3:22-cv-06987-JD](#)

ORDER RE MOTION TO DISMISS

Plaintiff Nathan Colombo sued defendants YouTube, LLC and Google LLC (collectively, YouTube) on behalf of himself and a putative class of Illinois residents for violating the Illinois Biometric Information Privacy Act (BIPA), 740 Ill. Comp. Stat. 14/1 *et seq.*¹ The operative second amended complaint (SAC) presents two claims alleging that YouTube violated Sections 15(a) and (b) of BIPA by collecting sensitive biometric identifiers and biometric information through its “Face Blur” and “Thumbnail Generator” video editing tools without first obtaining the necessary informed written consent or providing data retention and destruction policies to consumers. *See* Dkt. No. 84 ¶¶ 99-110.

YouTube has asked to dismiss the complaint under Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim. Dkt. No. 60. The motion is denied.

BACKGROUND

Launched in 2012, YouTube’s “Face Blur” tool uses facial recognition technology to enable its users, who create videos, to “select the faces’ in the user’s particular video that they

¹ The original named plaintiff was Brad Marschke. *See* Dkt. No. 1. After the briefing on this motion to dismiss was completed, Marschke asked to substitute Colombo as the named plaintiff, and the parties jointly requested that the Court deem “Nathan Colombo” to replace “Brad Marschke” in the briefing. Dkt. No. 82. The Court granted the requests, Dkt. No. 83, and Colombo filed a second amended class action complaint. The caption has been amended accordingly.

would ‘like to blur,’ which when applied and saved, will result in those faces appearing blurry and ostensibly unrecognizable to any viewer of the video.” Dkt. No. 84 ¶¶ 12, 49-50. According to the complaint, when the tool is deployed, YouTube “scan[s] the entire video to detect all unique faces within the video.” *Id.* ¶ 52. Through this process, YouTube captures and stores scans of face geometry from all detected faces, creating a unique “faceId” for each. *Id.* ¶ 55. The video creator can then “select which faces the creator would like to blur out in the video.” *Id.* ¶ 53. “[W]hen the ‘Face Blur’ tool is run multiple times on the same video, the previously stored result is provided to the user without actually rerunning the tool again,” even weeks after the initial run. *Id.* ¶ 58. Colombo alleges that YouTube permanently stores the scans of face geometry and does not disclose that they are collected and stored. *See id.* ¶¶ 59-60.

The “Thumbnail Generator” is “a feature that at first auto-generates photographic thumbnails (screenshots from an uploaded video) and allows creators to choose their own thumbnails for their videos.” *Id.* ¶ 64. Colombo says that “[i]t is common knowledge that thumbnails with faces, especially faces with more expression, generate more clicks and views.” *Id.* ¶ 65. YouTube is said to capitalize on this by scanning all videos for faces at the time they are uploaded and then using “this face data to auto-generate thumbnails that contain faces.” *Id.* ¶ 66. Through this process, YouTube “scan[s], detect[s], and collect[s] facial geometry within each YouTube video, including videos uploaded within Illinois, and then stor[es] the metadata associated with the videos.” *Id.* ¶ 71.

Colombo’s claims arise under BIPA. The Court has substantial familiarity with BIPA from *In re Facebook Biometric Information Privacy Litigation* and *Zellmer v. Facebook*, and has filed several detailed decisions that inform the discussion here.² In pertinent part, BIPA was enacted in 2008 and “manifests Illinois’ substantial policy of protecting its citizens’ right to privacy in their personal biometric data.” *In re Facebook Biometric Info. Privacy Litig.*, 185 F.

² *See In re Facebook Biometric Info. Privacy Litig.*, 326 F.R.D. 535 (N.D. Cal. 2018), *aff’d sub nom. Patel v. Facebook, Inc.*, 932 F.3d 1264 (9th Cir. 2019); *Patel v. Facebook Inc.*, 290 F. Supp. 3d 948 (N.D. Cal. 2018); *In re Facebook Biometric Info. Privacy Litig.*, No. 15-cv-03747-JD, 2018 WL 2197546 (N.D. Cal. May 14, 2018); *Zellmer v. Facebook, Inc.*, No. 18-cv-01880-JD, 2022 WL 976981 (N.D. Cal. Mar. 31, 2022); *Zellmer v. Facebook, Inc.*, No. 18-cv-01880-JD, 2022 WL 16924098 (N.D. Cal. Nov. 14, 2022).

Supp. 3d 1155, 1169 (N.D. Cal. 2016). “BIPA regulates the collection, retention, and disclosure of personal biometric identifiers and biometric information by ‘[m]ajor national corporations,’ among others.” *Id.* at 1171 (citing 740 Ill. Comp. Stat. 14/5(b), (g)). As BIPA requires:

(a) A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual’s last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.

(b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person’s or a customer’s biometric identifier or biometric information, unless it first:

(1) informs the subject or the subject’s legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;

(2) informs the subject or the subject’s legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

(3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject’s legally authorized representative.

740 Ill. Comp. Stat. 14/15. BIPA provides a private right of action to “[a]ny person aggrieved by a violation of” the statute. 740 Ill. Comp. Stat. 14/20.

LEGAL STANDARDS

The standards governing a Rule 12(b)(6) motion to dismiss are straightforward. *See McLellan v. Fitbit, Inc.*, No. 16-cv-00036-JD, 2018 WL 2688781, at *1 (N.D. Cal. June 5, 2018); *Jefferson v. Healthline Media, Inc.*, No. 22-cv-05059-JD, 2023 WL 3668522, at *1 (N.D. Cal. May 24, 2023). Rule 8(a)(2) requires that a complaint make “a short and plain statement of the claim showing that the pleader is entitled to relief.” Fed. R. Civ. P. 8(a)(2). To meet that rule and survive a Rule 12(b)(6) motion to dismiss, a plaintiff must allege “enough facts to state a claim to relief that is plausible on its face.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw

the reasonable inference that the defendant is liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Determining whether a complaint states a plausible claim for relief is a “context-specific task that requires the reviewing court to draw on its judicial experience and common sense.” *Id.* at 679.

DISCUSSION

I. BIOMETRIC IDENTIFIERS AND BIOMETRIC INFORMATION

YouTube’s kickoff objection is that Colombo has not plausibly alleged that the data collected from the Face Blur and Thumbnail Generator tools qualify as “biometric identifiers” or “biometric information” within the meaning of BIPA.³ See Dkt. No. 60 at 4. In YouTube’s view, biometric identifiers must identify a person and biometric information must actually be used to identify a person. See *id.* at 5-6. YouTube says that Colombo “does not allege a single fact that would plausibly lead” to the conclusion that the data it collects can be used to identify the individuals in the uploaded videos. *Id.* at 8.

The point is not well taken. BIPA defines “‘biometric identifier’ as ‘a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.’” *In re Facebook*, 185 F. Supp. 3d at 1171 (quoting 740 Ill. Comp. Stat. 14/10). “‘When a statute includes an explicit definition, we must follow that definition,’ even if it varies from a term’s ordinary meaning.” *Digital Realty Tr., Inc. v. Somers*, 138 S. Ct. 767, 776 (2018) (quoting *Burgess v. United States*, 553 U.S. 124, 130 (2008)); see also *People v. Fiveash*, 39 N.E.3d 924, 928 (Ill. 2015) (“When a term is defined within a statute, that term must be construed by applying the statutory definition provided by the legislature.”). The operative complaint plausibly alleges that YouTube’s Face Blur and Thumbnail Generator tools capture and store scans of face geometry, see Dkt. No. 84 ¶¶ 55, 59, 71, and YouTube does not demonstrate otherwise, see generally Dkt. Nos. 60, 79.

³ YouTube’s request for judicial notice, Dkt. No. 61, is granted with respect to Exhibits A and B, which are incorporated by reference in the complaint, and Exhibit C, consisting of legislative history. See *Anderson v. Holder*, 673 F.3d 1089, 1094 n.1 (9th Cir. 2012) (“Legislative history is properly a subject of judicial notice.”); *Shaw v. Ocwen Loan Servicing, LLC*, No. 15-cv-01755-JD, 2016 WL 7048979, at *2 (N.D. Cal. Dec. 5, 2016) (incorporation by reference). The request is denied with respect to Exhibit D, a news article about one company’s pre-BIPA collection and retention of biometric information, as it is not relevant to the resolution of this motion. See *Ruiz v. City of Santa Maria*, 160 F.3d 543, 548 n.13 (9th Cir. 1998).

YouTube’s request to ignore the definition of “biometric identifier” supplied by the Illinois legislature in favor of a single-minded focus on the word “identifier” is misdirected. YouTube says that a biometric identifier “must consist of, or at least link to, identity information (e.g., name, email address),” Dkt. No. 60 at 5, and that “reading the identification requirement out of ‘biometric identifier’ as [Colombo] urges would violate well-established canons of statutory construction that prohibit interpreting a statute in a way that would render portions of it superfluous,” Dkt. No. 79 at 2. In YouTube’s view, “[h]ad the Illinois General Assembly intended BIPA to apply to data whether or not it is in fact used to identify anyone, it easily could have omitted the reference to ‘identifiers’ altogether -- for example, by using terminology such as ‘biometric data,’ ‘biometric input,’ or simply ‘biometrics.’” *Id.* at 2-3. But the Illinois legislature was perfectly free to define “biometric identifier” in a specific manner that is not tethered to the plain meaning of the word “identifier” alone. *See, e.g., Tanzin v. Tanvir*, 141 S. Ct. 486, 490 (2020) (“[I]f a statute defines a ‘State’ to include territories and districts, that addition to the plain meaning controls.”). Nothing in the canons of statutory interpretation warrants a different conclusion.

YouTube’s suggestion that applying BIPA to the Face Blur and Thumbnail Generator tools would conflict with the statute’s intent, *see* Dkt. No. 60 at 8, is also unavailing. YouTube says “it would be impossible to locate and secure consent from everyone -- users and non-users alike -- whose face appears in a video on YouTube,” and that Colombo’s “interpretation of BIPA would effectively ban privacy-protective features like face blurring, an absurd result that the Illinois General Assembly cannot possibly have intended.” *Id.* at 8-9. But the named plaintiff whose claims are subject to this motion is a YouTube user who “has uploaded multiple videos to his YouTube account that include images of his face.” Dkt. No. 84 ¶ 83. Whether the putative class might properly include non-users whose faces appear in YouTube videos is a matter better suited to class certification proceedings. *See Milan v. Clif Bar & Co.*, 489 F. Supp. 3d 1004, 1008 (N.D. Cal. 2020).

II. EXTRATERRITORIALITY AND DORMANT COMMERCE CLAUSE

YouTube says that Colombo's claims would require an impermissible extraterritorial application of BIPA and that his interpretation of the statute would run afoul of the dormant Commerce Clause. *See* Dkt. No. 60 at 9-10. Neither argument is persuasive.

With respect to extraterritoriality, the parties agree that BIPA does not have extraterritorial reach because no "clear intent in this respect appears from the express provisions of the statute." *Avery v. State Farm Mut. Auto. Ins. Co.*, 835 N.E.2d 801, 852 (Ill. 2005) (internal quotations and citation omitted); *see* Dkt. No. 60 at 10; Dkt. No. 71 at 8. The salient inquiry is whether "the circumstances that relate to the disputed transaction occur[red] primarily and substantially in Illinois." *Avery*, 835 N.E.2d at 854. The thrust of YouTube's extraterritoriality argument is that Colombo does not allege that YouTube engaged in any relevant conduct in Illinois, such as maintaining servers in the state. *See* Dkt. No. 60 at 11-12.

The Court rejected a similar argument at the class certification stage in *In re Facebook*, and YouTube has cited no intervening authority that would counsel in favor of a different outcome here. *See In re Facebook Biometric Info. Privacy Litig.*, 326 F.R.D. 535, 547-48 (N.D. Cal. 2018). Colombo is an Illinois resident who has uploaded multiple videos to YouTube from within Illinois. *See* Dkt. No. 84 ¶ 22. His claims are based on the application of Illinois law to use of YouTube in Illinois. The provision of access and services to Colombo and other Illinois users constitutes in-state activity by YouTube. *See Vance v. Microsoft Corp.*, No. 20-cv-01082-JLR, 2022 WL 9983979, at *7 (W.D. Wash. Oct. 17, 2022) (discussing *In re Facebook* and observing that "Facebook reached into Illinois by providing its service to the plaintiffs, and the plaintiffs' direct interactions with Facebook gave rise to the alleged BIPA violations"). While YouTube's headquarters and data servers may be elsewhere, that is not dispositive. "Making the geographic coordinates of a server the most important circumstance in fixing the location of an Internet company's conduct would yield . . . questionable results" and "effectively gut the ability of states without server sites to apply their consumer protection laws to residents for online activity that occurred substantially within their borders." *In re Facebook*, 326 F.R.D. at 548.

1 YouTube’s dormant Commerce Clause theory fares no better. The Supreme Court “has
 2 held that the Commerce Clause not only vests Congress with the power to regulate interstate trade;
 3 the Clause also ‘contain[s] a further, negative command,’ one effectively forbidding the
 4 enforcement of certain state [economic regulations] even when Congress has failed to legislate on
 5 the subject.” *Nat’l Pork Producers Council v. Ross*, 143 S. Ct. 1142, 1152 (2023) (alterations in
 6 original) (quoting *Okla. Tax Comm’n v. Jefferson Lines, Inc.*, 514 U.S. 175, 179 (1995)). The
 7 dormant Commerce Clause “typically applies when a state tries to regulate or control economic
 8 conduct wholly outside its borders with the goal of protecting local businesses from out-of-state
 9 competition.” *In re Facebook Biometric Info. Privacy Litig.*, No. 15-cv-03747-JD, 2018 WL
 10 2197546, at *4 (N.D. Cal. May 14, 2018) (citing *Healy v. Beer Inst., Inc.*, 491 U.S. 324, 336-37
 11 (1989)). It is a “limitation upon the power of the States” intended to prohibit “discrimination
 12 against interstate commerce” and “state regulations that unduly burden interstate commerce.” *Sam*
 13 *Francis Found. v. Christies, Inc.*, 784 F.3d 1320, 1323 (9th Cir. 2015) (en banc) (internal
 14 quotations and citations omitted).

15 YouTube again urges a point rejected in *In re Facebook*, and has not said why a different
 16 outcome might be appropriate in this case. “[T]he application of BIPA to Illinois users does not
 17 have the impermissible “‘practical effect” of regulating commerce occurring wholly outside’
 18 Illinois.” *In re Facebook*, 2018 WL 2197546, at *4 (quoting *Healy*, 491 U.S. at 332). As
 19 discussed above, YouTube’s allegedly BIPA-violating conduct “cannot be understood to have
 20 occurred wholly outside Illinois, and the same rather metaphysical arguments about where BIPA
 21 was violated fare no better when re-packaged under” the dormant Commerce Clause. *Id.*
 22 YouTube suggests that this case is “indistinguishable” from *Christies*, Dkt. No. 79 at 8, where the
 23 Ninth Circuit held that a provision of a California law that regulated sales of fine art conducted
 24 entirely outside of the state violated the dormant Commerce Clause, *see Christies*, 784 F.3d at
 25 1323-25. Not so. This case arises from an Illinois resident’s interactions with YouTube from
 26 within his home state and consequently “is deeply rooted in BIPA’s native soil of Illinois.” *In re*
 27 *Facebook*, 2018 WL 2197546, at *4.


III. THE SECTION 15(a) CLAIM

YouTube’s closing argument is that the Section 15(a) claim should be dismissed because Colombo “has not pleaded facts establishing that he is ‘aggrieved’ by [YouTube’s] alleged violation of that section,” Dkt. No. 60 at 14, as is required to bring a claim under BIPA. Section 15(a) provides, in pertinent part, that a “private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information.” 740 Ill. Comp. Stat. 14/15(a). Under Illinois law, “a party is aggrieved by an act that directly or immediately affects her legal interest.” *In re Facebook*, 326 F.R.D. at 546 (citing *Am. Sur. Co. v. Jones*, 51 N.E.2d 122 (Ill. 1943)).

Colombo says that YouTube “failed to develop or implement a BIPA-compliant data collection policy,” and “therefore failed to comply with any BIPA-compliant policy in [its] handling of [his] personally identifying information.” Dkt. No. 84 ¶ 86 (emphases omitted). At the pleadings stage, this is enough to move forward. While “‘the duty to disclose’ a written policy under Section 15(a) ‘is owed to the public generally, not to particular persons whose biometric information the entity collects,’” *Zellmer v. Facebook, Inc.*, No. 18-cv-01880-JD, 2022 WL 16924098, at *3 (N.D. Cal. Nov. 14, 2022) (quoting *Bryant v. Compass Grp. USA, Inc.*, 958 F.3d 617, 626 (7th Cir. 2020)), Colombo plausibly alleges that his privacy interests have been directly affected by YouTube’s conduct in not complying with a data-retention policy in handling his data.

IT IS SO ORDERED.

Dated: June 28, 2023



JAMES DONATO
United States District Judge